



Denise Yee
Senior Trademark Counsel
Visa Legal Department
yee@visa.com

**The Department of Commerce
United States Patent and Trademark Office
National Telecommunications and Information Administration**

Docket No. 10090448-0448-01

**Inquiry on Copyright Policy, Creativity, and Innovation in the Internet
Economy**

COMMENTS OF VISA INC.

Visa Inc. welcomes the opportunity to provide its views on the challenges of protecting copyrighted works online and the relationship between copyright law and innovation in the Internet economy. Visa supports strong enforcement of intellectual property rights. The “VISA” trademark is one of Visa’s most important assets, and is considered among the strongest brands in the world. Visa expends hundred of thousands of dollars protecting and enforcing the “VISA” brand.

Recognizing the difficulty of protecting intellectual property rights in the digital environment, Visa willingly assists copyright owners in this effort. However, four principles guide this assistance:

- The copyright owners bear the primary responsibility for protecting their copyrights.
- Protection of copyrights in the digital environment should not be achieved in a manner that places an undue burden on the processing of electronic commerce transactions.

- Visa does not bear secondary copyright liability for the use of its payment system to purchase allegedly infringing materials.
- Visa can assist in disrupting the infringing activity, but it is not in a position to permanently stop the activity.

In these comments, Visa will provide a brief overview of its operations and structure. It will then discuss *Perfect 10 v. Visa International Service Association*, where the Ninth Circuit held that Visa and other payment systems were not secondarily liable for the use of their networks to purchase infringing material from websites. Next, the comments will describe the efforts Visa undertook voluntarily to prevent the use of its payment system by the Russian website AllofMP3.com, and the liability and legal costs it and its partner bank incurred as a result. The comments will proceed to discuss Visa's current policy for responding to complaints by copyright owners concerning websites selling infringing material, and the best practices developed by payment system industry players to address this issue. Finally, the comments will offer recommendations for policy-making in this area.

I. The Visa Network

Visa Inc. is a global company headquartered in San Francisco, California. The company's operating regions include: Asia-Pacific; Canada; Central and Eastern Europe, Middle East and Africa; Latin America and the Caribbean; and USA. Visa Europe is a separate entity that is an exclusive licensee of Visa Inc.'s trademarks and technology in the European region.¹

¹ Visa Europe is owned and operated by more than 4,000 European member banks and was incorporated in July 2004. In October 2007, Visa Europe became independent of global Visa Inc., with an exclusive, irrevocable and perpetual licence in Europe.

Visa operates a global electronic payments network. Visa facilitates global commerce through the transfer of value and information among financial institutions, merchants, consumers, businesses and government entities in more than 200 countries and territories worldwide.

Visa provides its financial institution clients with a broad range of platforms for consumer credit, debit, prepaid and commercial payments. Visa's network and payment platforms deliver significant value to our clients and their customers in terms of greater efficiency, security, convenience and global reach. Visa does not issue cards, set cardholder fees or interest rates or arrange for merchant acceptance of Visa cards. These relationships are managed by our network of more than 15,700 financial institution clients worldwide.

A court recently described the credit card transaction process for the Visa and MasterCard networks as follows:

A customer will initiate the process when he or she purchases a product from the merchant with a credit card. Once the credit card information is "swiped" on a terminal, or entered on a website, the merchant terminal transmits an authorization request to the merchant's "acquiring bank...." The acquiring bank sends the credit card request through [the Visa or MasterCard] electronic network to the cardholder's issuing bank. Based on the cardholder's credit limit or other factors, the issuing bank will send a message back through the network to the acquiring bank, who forwards it back to the merchant, which states that the merchant should either approve or decline the transaction. If approved, the merchant will complete the transaction and the acquiring bank will credit the merchant's account with the appropriate amount of funds. This entire process typically takes a matter of seconds. Some days to months after the sale is completed, the acquiring bank will submit the transaction information to the issuing bank, which will seek payment from the cardholder and settle with the acquiring bank.

Gucci America, Inc. v. Frontline Processing Corp., 2010 U.S. Dist. LEXIS 62654 (S.D.N.Y. June 23, 2010).

In 2010, Visa conducted more than \$5 trillion worth of business and processed 68.4 billion transactions. The 1.8 billion cards issued by our 15,700 financial institution clients are accepted at millions of merchant outlets and over a million ATMs worldwide.

To promote growth in this channel of commerce, to protect the Visa brand and because it is the right thing to do, Visa goes beyond any legal requirements to prevent the use of its payment system for illegal electronic commerce transactions. Visa policy is unequivocal and clear: its system should not be used for illegal transactions.

Visa works cooperatively with law enforcement in the United States and around the world to aid their law enforcement efforts. Visa takes special steps in cases of criminal activity and activity that threatens health and safety. For example, Visa searches the Internet for merchants selling or advertising child pornography or illegally distributing controlled substances and expels them from our system as soon as they are discovered. Visa works cooperatively with law enforcement, other payment brands and the National Center for Missing and Exploited Children in the Financial Coalition Against Child Pornography to share information and take collaborative steps against child pornography merchants.

Visa works with the Secret Service, the FBI, the Federal Trade Commission, and state Attorneys General to assist their efforts to stop fraud, identity theft, and data breaches. Visa has worked with the Department of Justice and State Attorneys General to respond to their concerns about illegal online tobacco merchants. Finally, in response to the Unlawful Internet Gambling Enforcement Act (UIGEA), Visa devised a coding

and blocking scheme that prevents U.S. cardholders from engaging in illegal Internet gambling while also allowing offshore gambling merchants to provide service to cardholders in jurisdictions where Internet gambling is legal.

The task of preventing illegal transactions is complicated by Visa's corporate structure. Visa does not have a direct business relationship with merchants. Rather, it is the acquiring financial institution that establishes contractual relationships with merchants and is ultimately responsible for monitoring their processing activity. As a result, Visa must locate the bank that manages the merchant account. In the case of an offshore merchant, this will involve working closely with regional Visa Inc. officials or officials at the separate entity, Visa Europe, who have responsibility for that acquiring bank. Once Visa notifies the bank of the illegal activity, that usually resolves the issue. In most cases, the bank does not want the business and terminates the merchant or takes other action to bring the merchant into compliance with our policies. If the transaction is clearly illegal and the bank does not take action, Visa can take further enforcement action against the bank.

II. Secondary Copyright Liability – *Perfect 10 v. Visa*

In *Perfect 10 v. Visa International Service Association*, 494 F.3d 788 (9th Cir. 2007), the U.S. Court of Appeals for the Ninth Circuit held that payment systems do not bear secondary copyright liability for the use of their networks by websites selling infringing material. Because *Perfect 10* defines the scope of payments systems' liability for third party infringement, it merits detailed attention.

Perfect 10 is a publisher of adult magazines and websites. Perfect 10 believed that operators of other websites had, without authorization, copied images from the Perfect 10

website and then displayed the copied images on their websites. Rather than bring infringement actions against the website operators, Perfect 10 initiated a series of suits against a variety of intermediaries, including web hosts, search engines, and payment systems, for facilitating the infringement. The courts rejected Perfect 10's claims.²

In its action against Visa, MasterCard, and other providers of payment services, Perfect 10 claimed that by providing payment services to websites selling images that infringed Perfect 10's copyrights, the payment systems were secondarily liable for copyright infringement.³ The district court granted the payment systems' motion to dismiss Perfect 10's complaint. On appeal, the Ninth Circuit found that Visa and the other defendants were not liable for either contributory infringement or vicarious liability.⁴

A. Contributory Infringement

The Ninth Circuit laid out the following test for contributory infringement: "one contributorily infringes when he 1) has knowledge of another's infringement and 2) either a) materially contributes to or b) induces that infringement." 494 F.3d at 795. The court ruled that the payment systems did not materially contribute to the infringement because "they have no direct connection" to the infringement. The court reviewed its precedents where it found material contribution, *e.g.*, *Fonovisa v. Cherry Auction*, 76 F.3d 259 (9th Cir. 1996), *A & M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001), and

² See also *Perfect 10 v. CCBill*, 488 F.3d 1102 (9th Cir. 2007); *Perfect 10 v. Amazon.com*, 508 F.3d 1146 (9th Cir. 2007). Although the defendants in *CCBill* also provided payment services, the litigation focused on the applicability of the safe harbors under the Digital Millennium Copyright Act, and never reached the underlying issue of secondary copyright liability.

³ Perfect 10 also brought claims for trademark infringement and state law claims for false advertising and unfair competition. Perfect 10 lost on these claims as well.

⁴ Judge Alex Kozinski dissented from the majority decision.

Perfect 10 v. Amazon.com, 508 F.3d 1146 (9th Cir. 2007), and in each case noted that the defendant had some nexus to the reproduction, display, or distribution of the infringed works. By contrast, the payment systems had no involvement in these activities. While “Defendants make it easier for websites to profit from this infringing activity, the issue here is reproduction, alteration, display, and distribution, which can occur without payment.” 494 F.3d at 796.

After discussing material contribution, the court briefly turned to the issue of inducement. It reviewed the Supreme Court’s holding in *MGM v. Grokster*, 545 U.S. 913 (2005), and concluded that there were no affirmative acts or clear expression by the payment systems that showed any specific intent to foster infringement.

B. Vicarious Liability

With respect to vicarious liability, the court found that the payment systems had no practical ability to prevent the infringing activity, because the websites could continue to operate even if the companies excluded them from their payment systems. “Defendants can block access to their payment system, but they cannot themselves block access to the Internet, to any particular website, or to search engines enabling location of such websites.” 494 F. 3d at 804. The court acknowledged that the companies could exert financial pressure on the websites, “[b]ut the ability to exert financial pressure does not give Defendants the right or ability to control the actual infringing activity in this case. Defendants have no absolute right to stop that activity – they cannot stop websites from reproducing, altering, or distributing infringing images.” *Id.* at 804-05. The court further noted that many other entities had the ability to exert indirect pressure on website operators, including search engines and utility companies.

The court also discussed the liability of the banks that had the contractual relationships with the infringing merchants. These banks, too, were defendants in this case. The court noted that even though these banks, unlike Visa and MasterCard, had a direct relationship with the infringing merchants, the activities of these banks did not constitute personal participation in the infringing activity: these banks “are not personally involved in the reproduction, alteration, or distribution of the infringing images. Rather, they merely process payments related to those activities.” *Id.* at 809 n. 20.⁵

III. AllofMP3.com

Notwithstanding the unambiguous holding of the Ninth Circuit that payment systems do not have secondary copyright liability for the infringing activities of websites that use their services, Visa has voluntarily elected to assist copyright owners address the problem of websites selling infringing content. Proving the accuracy of the adage that no good deed goes unpunished, this assistance proved costly to Visa in the Allofmp3.com case.

⁵ The Ninth Circuit recognized that Visa and MasterCard have no contractual relationship with the individual website operators. The court cited a case that turned on the fact that Visa did not interact directly with cardholders or merchants, but instead acted as a clearinghouse between these banks with the merchant accounts and the banks that issue credit cards to consumers. *Emery v. Visa International Service Association*, 95 Cal. App. 4th 952, 116 Cal. Rptr. 2d (2002). The district court in *Gucci America, Inc. v. Frontline Processing Corp.*, 2010 U.S. Dist. LEXIS 62654 (S.D.N.Y. June 23, 2010), refused to dismiss secondary trademark infringement claims against an acquiring bank and independent service organizations that provided payments services to a website that sold counterfeited goods. The court stated that “[w]hile in *Perfect 10* the credit card services may not have been needed for a website to display infringing photographs, the infringement here occurred through the sale of the counterfeit products” that could not have transpired but for the participation of the defendants. *Id.* at *12.

In 2006, Visa officials received a documented complaint by copyright owners that the Russian website AllofMP3.com was infringing on their copyrights by allowing downloads of music without having obtained the authorization of the copyright owners. Visa conducted an assessment of legal situation, including a review by outside counsel, and concluded that under local Russian law and under the laws of the vast majority of the merchant's consumers – located primarily in the United States and Great Britain – the merchant's transactions were illegal. After appropriate notice, the Russian bank working with Allofmp3.com stopped processing Visa transactions at the end of September 2006. When the merchant began routing transactions through an affiliated site called Alltunes, the bank cut off transactions from that site as well.

The common owner of both affiliated sites sued the bank in a Russian court. Visa intervened in the case as a third party in support of the bank. In June 2007, the Russian court found in favor of the merchant concluding the bank was in violation of its contract with the merchant, and the bank and Visa were ordered to continue to provide processing services. In response to the bank's claim that the merchant was acting illegally and so in violation of Visa rules, the court found that no Russian court had determined that the merchant was infringing any copyright in Russia. While some record companies had brought a separate copyright infringement action in Russia against the owner of these sites, that court had not yet rendered a judgment as of June 2007, when the first court found that the bank had breached its contract with the websites' owner.

Subsequently, in August 2007, the second court ruled against the record companies in the separate copyright infringement action. That court held that Allofmp3.com and similar downloading music sites were legal in Russia. Even though

the copyright owners had not given permission to the site to sell copies of their music, a Russian collective management organization had the right to license use of the sound recordings. The court determined that Allofmp3.com and its affiliates were in compliance with Russian law to the extent that they paid for rights from this organization.

These court cases created a serious challenge for Visa. Visa responded to a fully documented complaint of copyright infringement from the copyright owner, but the local courts ordered the local client bank to continue to provide service. However, these transactions would still be illegal under the laws in virtually every other country in the world. Visa decided to allow the local Russian bank to provide only domestic service to the particular Russian download site involved in the court case. International transactions from customers in other countries would not be allowed.

Visa learned three important lessons from this case:

First, Visa learned the limits of private sector enforcement efforts in cases of international infringement. Copyright law is extremely complex, and the opinions of the copyright owners or Visa concerning the lawfulness of a use are just that – opinions. In this case, the foreign court ultimately disagreed with the opinions of our lawyers and the copyright owners’ lawyers. As a result, Visa’s client bank was exposed to legal liability for withdrawing service to merchants found to be operating properly within local law. Visa simply is not in a position to override local law in these circumstances.

Second, Visa learned that when local laws are not consistent, governments and aggrieved businesses cannot put private sector intermediaries like Visa in the position of resolving the conflicts. Ultimately resolving these issues require government-to-government discussions that harmonize local legal structures. It is only within these

harmonized legal structures that private enforcement efforts such as Visa's can fully succeed.

Third, Visa learned that it had to develop a policy to deal with copyright infringement. It could have decided that consistent with the absence of legal responsibility under *Perfect 10*, it would simply process transactions for merchants within the system, and inform copyright owners that their redress was to sue the infringing merchant in its jurisdiction. Instead, it adopted the following global policy: "a transaction must be legal in both the Cardholder's jurisdiction and the Merchant's jurisdiction."

IV. Visa's Current Policy

This policy requiring a transaction to be lawful in both the seller's and the buyer's jurisdiction is still in effect today.⁶ Under Visa's current procedures, upon notification by a copyright holder of the illegal activity, Visa will notify the acquiring bank (the bank that has the business relationship with the merchant) and require the acquiring bank to investigate the claim of illegal transactions to ensure that no prohibited transactions are entered into the Visa system by the offending merchant. The policy also sets forth a schedule of fines and penalties against the acquiring bank to ensure compliance.

This policy applies to all illegal cross-border transactions, not only to online copyright infringement. It has been employed successfully to diminish the number of identified websites from using the Visa network to receive payment for child pornography, drug trafficking, money laundering, and other illegal conduct.

Recently, in fact, a motion picture studio informed Visa of ten websites that were

⁶ If the buyer and the seller are in the same jurisdiction, Visa will process the transaction if it is lawful under local law.

suspected of engaging in illegal activity and accepting Visa as a form of payment. Visa promptly implemented its procedures, and within days of notification, the applicable acquiring banks began investigating these sites, and as necessary, terminated payment services to these sites, or brought their merchants into compliance.

Additionally, Visa has collaborated with MasterCard, American Express, Discover, and PayPal to develop “Best Practices to Address Copyright Infringement and the Sale of Counterfeit Products on the Internet.” These best practices demonstrate the payment industry’s commitment to work with copyright owners to prevent the distribution of infringing content through the Internet.

Unfortunately, few copyright owners have availed themselves of Visa’s procedures, or other payment system’s procedures.

V. Policy Recommendations

Visa has the following recommendations to the USPTO and the NTIA as they develop policies to address the problem of copyright infringement online.

- The Ninth Circuit’s holding in *Perfect 10 v. Visa* should not be disturbed. Visa and other payment systems are too far removed from the infringing conduct to be treated as secondary infringers.
- Copyright owners should bear the cost of protecting their rights. Proposed legislation in Canada would allow the government to set a maximum fee to be paid by copyright owners for using the legislation’s “notice and notice” system. Similarly, copyright owners will bear 75% of Internet service providers’ costs of complying with the graduated response requirements of the United Kingdom’s 2010 Digital Economy law. Copyright owners should be willing to indemnify

payment systems for any liability they incur as a result of actions taken to protect the interests of copyright owners. Similarly, copyright owners should be willing to reimburse payment systems for the cost of responding to copyright owner complaints regarding infringement.

- Payment systems are not in a position to assess the viability of a copyright owner's claim, or the legality of a merchant's activity.
- Requiring payment systems to cease providing payment services to merchants operating infringing websites should not be viewed as an effective solution to permanently eliminate online infringement. Merchants engaged in illegal activity often have accounts with several different financial institutions under several different names. As soon as one acquiring bank stops providing payment services to the merchant, the merchant starts using another account under a different name at a different acquiring bank. As noted above, there are over 16,400 financial institutions in the Visa network. This provides the unscrupulous merchant with many alternatives to stay in business, notwithstanding Visa's best efforts.
- If legal obligations are placed on payment systems to cease providing payment services to infringing websites, policy makers should ensure that the payments systems are not subject to conflicting legal obligations. Such conflicts are most likely to arise in cross-border transactions. For example, a U.S. statute might require a payment system to stop processing transactions for a website determined by a U.S. court to infringe U.S. copyright laws, but the payment system (or the foreign acquiring bank with the actual business relationship with the website operator) could have a contractual obligation to provide services to the website

operator. If the payment system or the acquiring bank ceased providing payment services to the website, the website operator could sue the payment system or its acquiring bank in the country where the website is hosted, and where that activity might be considered legal. In the absence of a finding that the website infringed that jurisdiction's copyright law, the foreign court could very well rule that the payment system or the acquiring bank breached its contractual obligation to provide payments services to the website operator. (This is precisely what happened in the *AllofMP3* case discussed above.)

- Extraterritorial application of U.S. law will invite similar measures by other countries. If U.S. law makes payment systems instruments of U.S. copyright enforcement actions against foreign websites, foreign governments are sure to do the same. European countries, for example, believe that many U.S. companies infringe European laws concerning geographical indicators. Under European law, only wineries in the Champagne region of France can call sparkling wine "champagne," and only cheese manufacturers in the Parma region of Italy can use the name "parmesan cheese." European countries could require payment systems to stop processing transactions for U.S. websites that sell products that violate European laws concerning geographical indicators. Similarly, repressive governments could force payment systems to stop doing business with U.S. websites that sell books critical of their regimes.
- Policies that combat online infringement should be adopted only if the likely benefit clearly outweighs the possible harm to electronic commerce. Over the past twenty years, attempts to use legal mechanisms to prevent online

infringement have met with only limited success. At the same time, the Internet has grown into a major channel of commerce both in the United States and abroad. Payment systems such as Visa have facilitated the use of the Internet for commerce by providing a secure, familiar, and efficient means for consumers to purchase goods and services from websites operated by a wide variety of merchants around the globe. Copyright enforcement obligations that interfere with this activity should not be placed on payment systems.

Respectfully submitted,

Denise Y. Yee
Senior Trademark Counsel
Visa Legal Department
yee@visa.com

December 10, 2010